18.783 Elliptic Curves **Spring 2013**
Problem Set #9 **Due: 04/25/2013**

Description

These problems are related to the material covered in Lectures 18-19. As usual, the first person to spot each non-trivial typo/error will receive a point of extra credit.

Instructions: Either solve both problems 1 and 2, or solve just problem 3, and then complete Problem 4, which is a survey. **Late problem sets will lose half a point for each hour they are late**.

Problem 1. Complex multiplication (40 points)

Let $\tau = (1 + \sqrt{-7})/2$. In problem 1 of Problem Set 8 you computed $j(\tau) = -3375$. In problem 2 of Problem Set 7 you proved that the endomorphism ring of the elliptic curve $y^2 = x^3 - 35x - 98$ (with j-invariant -3375) is isomorphic to $[1, \tau]$, the maximal order of $\mathbb{Q}(\sqrt{-7})$. We now set $g_2 = -4(-35) = 140$ and $g_3 = -4(-98) = 392$ and work with the isomorphic elliptic curve $E/\mathbb{C}$ defined by

$$y^2 = 4x^3 - g_2x - g_3.$$

We should note that $g_2([1, \tau])$ and $g_3([1, \tau])$ are not equal to 140 and 392, but there is a lattice L for which $g_2(L) = 140$ and $g_3(L) = 392$ (you computed L in problem 2 of Problem Set 8), and L is homothetic to $[1, \tau]$. In particular, $\tau L \subseteq L$, thus τ satisfies condition (1) of Theorem 18.7. The goal of this problem is to compute the polynomials $u, v \in \mathbb{C}[x]$ for which condition (2) of Theorem 18.7 holds, and the endomorphism ϕ for which condition (3) of Theorem 18.7 holds, and to explicitly confirm that the diagram

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{\ \Phi\ } & E(\mathbb{C}) \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \phi} \\ \mathbb{C}/L & \xrightarrow{\ \Phi\ } & E(\mathbb{C}) \end{array}$$

commutes, where τ denotes the multiplication-by-τ map $z \mapsto \tau z$.

Recall that the Weierstrass $\wp$-function satisfying the differential equation

$$(\wp(z)')^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3 \tag{1}$$

has a Laurent series expansion about 0 of the form $\wp(z) = z^{-2} + \sum_{n=1}^{\infty} a_{2n}z^{2n}$.

1. Use g_2 and g_3 to determine a_2 and a_4, and then determine a_6 by comparing coefficients in the Laurent expansions of both sides of (1).

We now wish to compute the polynomials $u, v \in \mathbb{C}[x]$ for which

$$\wp(\tau z) = \frac{u\big(\wp(z)\big)}{v\big(\wp(z)\big)},$$

as in condition (2) of Theorem 18.7. We have $N(\tau) = \tau\bar{\tau} = 2$, so $\deg u = 2$ and $\deg v = 1$. We can make $u = x^2 + ax + b$ monic, and with $v = cx + d$ we must have

$$(c\wp(z) + d)\wp(\tau z) = \wp(z)^2 + a\wp(z) + b \tag{2}$$

2. Use (2) to determine the coefficients a, b, c, d, expressing your answers in terms of τ. It will be convenient to work in the subfield $K = \mathbb{Q}(\tau)$, rather than $\mathbb{C}$. To define the field K and the polynomial ring $K[x]$ in Sage, use

```
RQ.<w>=PolynomialRing(QQ)
K.<tau>=NumberField(w^2-w+2)
RK.<x>=PolynomilaRing(K)
```

Once you have determined $a, b, c, d \in K$, you can verify $u, v \in K[x]$ via[1]

```
wp=EllipticCurve([-35,-98]).weierstrass_p(100).change_ring(K)
assert wp(tau*z) == u(wp)/v(wp)
```

3. Following the proof of Theorem 18.7, construct polynomials $s, t \in K[x]$ that satisfy

$$\wp'(\tau z) = \frac{s\big(\wp(z)\big)}{t\big(\wp(x)\big)}\wp'(z).$$

You can verify your results in Sage via

```
assert wp.derivative()(tau*z) == s(wp)/t(wp)*wp.derivative()
```

4. Now let $\phi = \big(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\big)$. Use Sage to verify that ϕ is an endomorphism by checking that its coordinate functions satisfy the curve equation $y^2 = 4x^3 - g_2x - g_3$.

The symbolic verifications in parts 2 and 4 confirm that $\Phi(\tau z) = \phi(\Phi(z))$, showing that the diagram commutes (at least for the first 100 terms in the Laurent expansion of $\wp(z)$). But we would like to explicitly check this for some specific values of $z \in \mathbb{C}$. In order to do this in Sage, we need to redefine τ and the polynomials u, v, s, t over $\mathbb{C}$, rather than K. Use the following Sage script to do so

```
R.<X>=PolynomialRing(CC)
pi=K.embeddings(CC)[0]
tauC=pi(tau)
uC=sum([pi(u.coeffs()[i])*X^i for i in range (0,u.degree()+1)])
vC=sum([pi(v.coeffs()[i])*X^i for i in range (0,v.degree()+1)])
sC=sum([pi(s.coeffs()[i])*X^i for i in range (0,s.degree()+1)])
tC=sum([pi(t.coeffs()[i])*X^i for i in range (0,t.degree()+1)])
```

5. Pick three "random" nonzero complex numbers z_1, z_2, z_3 of norm less than 0.1 (they need to be close to 0 in order for the Laurent series of $\wp(x)$ to converge quickly). You can approximate the point $P_1 = \Phi(z_1) = \big(\wp(z_1), \wp'(z_1)\big)$ on the elliptic curve $y^2 = 4x^3 - g2x - g3$ in Sage using

```
wp = EllipticCurve([CC(-35),CC(-98)]).weierstrass_p(100)
P1=(wp(z1),wp.derivative()(z1))
```

[1] Sage effectively computes $\wp(z)$ using $y^2 = 4x^3 - g_2x - g_3$ when we define $E\colon y^2 = x^3 + Ax + B$ with $g_2 = -4A$ and $g_3 = -4B$.

For $i = 1, 2, 3$, compute the points $P_i = \Phi(z_i)$ and $Q_i = \Phi(\tau z_i)$ (remember to use the embedding of τ in $\mathbb{C}$). Check that the points all approximately satisfy the curve equation $y^2 = 4x^3 - g_2 x - g_3$ (if not, use z_i with smaller norms). Then verify that Q_i and $\phi(P_i)$ are approximately equal in each case.

Problem 2. Binary quadratic forms (60 points)

A *binary quadratic form* is a homogeneous polynomial of degree 2 in two variables:

$$f(x, y) = ax^2 + bxy + cy^2,$$

which we identify by the triple (a, b, c). We are interested in a specific set of binary quadratic forms, namely, those that are *integral* ($a, b, c \in \mathbb{Z}$), *primitive* ($\gcd(a, b, c) = 1$), and *positive definite* ($b^2 - 4ac < 0$ and $a > 0$). Henceforth we shall use the word *form* to refer to an integral, primitive, positive definite, binary quadratic form. The *discriminant* of a form is the negative integer $D = b^2 - 4ac$, which is necessarily congruent to 0 or 1 mod 4. We generically call such integers (imaginary quadratic) discriminants, and let $F(D)$ denote the set of forms with discriminant D.

1. Prove that $\mathrm{SL}_2(\mathbb{Z})$ acts on the set $F(D)$ via

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix} f(x, y) = f(sx + ty, ux + vy).$$

Forms f and g are (properly) *equivalent* if $g = \gamma f$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. In this problem and the next, you will prove that the set $\mathrm{cl}(D)$ of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of $F(D)$ forms a finite abelian group, and develop algorithms to compute in this group.

The group $\mathrm{cl}(D)$ is called the *class group*, and it plays a key role in the theory of complex multiplication. Our first objective is to prove that $\mathrm{cl}(D)$ is finite, and to develop an algorithm to enumerate unique representatives of its elements (which also allows us to determine its cardinality). We define the (principal) *root* τ of a form $f = (a, b, c)$ to be the unique root of $f(x, 1)$ in the upper half plane:

$$\tau = \frac{-b + \sqrt{D}}{2a}.$$

Recall that $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half plane $\mathbb{H}$ via linear fractional transformations

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix} \tau = \frac{s\tau + t}{u\tau + v},$$

and that the set

$$\mathcal{F} = \left\{\tau \in \mathbb{H} : \mathrm{re}(\tau) \in [-1/2, 0] \text{ and } |\tau| \geq 1\right\} \cup \left\{\tau \in \mathbb{H} : \mathrm{re}(\tau) \in (0, 1/2) \text{ and } |\tau| > 1\right\}$$

is a fundamental region for $\mathbb{H}$ modulo the $\mathrm{SL}_2(\mathbb{Z})$-action.

2. Prove that $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ acts (anti-)compatibly on forms and their roots by showing that if τ is the root of f, then $\gamma^{-1}\tau$ is the root of γf. Conclude that two forms are equivalent if and only if their roots are equivalent.

The form $f = (a, b, c)$ is *reduced* if

$$-a < b \leq a < c \qquad \text{or} \qquad 0 \leq b \leq a = c.$$

3. Prove that a form is reduced if and only if its root lies in the fundamental region $\mathcal{F}$. Conclude that each equivalence class in $F(D)$ contains exactly one reduced form.

4. Prove that if f is reduced then $a \leq \sqrt{|D|/3}$. Conclude that the set $\mathrm{cl}(D)$ is finite, and show that in fact its cardinality $h(D)$ satisfies $h(D) \leq |D|/3$. Prove that $F(D)$ contains a unique reduced form (a, b, c) with $a = 1$. Thus $h(D) \geq 1$, which proves that $h(-3) = h(-4) = 1$.

The positive integer $h(D)$ is called the *class number* of the discriminant D.

5. Give an algorithm to enumerate the reduced forms in $F(D)$. Using the upper bound $h(D) = O(|D|^{1/2} \log |D|)$, prove that your algorithm runs in $O(|D|\mathsf{M}(\log |D|))$ time.

6. Implement your algorithm and use it to enumerate the five reduced forms in $F(-103)$ and the six reduced forms in $F(-396)$. Then use it to compute $h(D)$ for the first three discriminants $D < -N$, where N is the integer formed by the first four digits of your student ID.

Problem 3. The class group (100 points)

In Problem 2 it was proved that $\mathrm{cl}(D)$ is a finite set. In this problem you will prove that it is an abelian group, and develop an algorithm to implement the group operation.

To each form $f(x, y) = ax^2 + bxy + cy^2$ in $F(D)$ with root $\tau = (-b + \sqrt{D})/(2a)$, we associate the lattice $L(f) = L(a, b, c) = a[1, \tau]$.

1. Show that two forms $f, g \in F(D)$ are equivalent if and only if the lattices $L(f)$ and $L(g)$ are homothetic.

For any lattice L, the *order* of L is the set

$$\mathcal{O}(L) = \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}.$$

2. Prove that either $\mathcal{O}(L) = \mathbb{Z}$ or $\mathcal{O}(L)$ is an order in an imaginary quadratic field, and that homothetic lattices have the same order. Prove that if L is the lattice of a form in $F(D)$, then $\mathcal{O}(L)$ is the order of discriminant D in the field $K = \mathbb{Q}(\sqrt{D})$.

For the rest of this problem let $\mathcal{O}$ denote the (not necessarily maximal) imaginary quadratic order of discriminant D, which may be represented as a lattice $L = [1, \alpha]$, where α is any algebraic integer whose minimal polynomial $x^2 + bx + c$ has discriminant $b^2 - 4c = D$.

Recall that an (integral) $\mathcal{O}$-*ideal* $\mathfrak{a}$ is an additive subgroup of O that is closed under multiplication by $\mathcal{O}$. Every $\mathcal{O}$-ideal $\mathfrak{a}$ is necessarily a sublattice of $\mathcal{O}$, and its *norm* $N(\mathfrak{a})$ is the index $[\mathcal{O} : \mathfrak{a}] = |\mathcal{O}/\mathfrak{a}|$. An $\mathcal{O}$-ideal $\mathfrak{a}$ is said to be *proper* if $\mathcal{O}(\mathfrak{a}) = \mathcal{O}$. Note that we always have $\mathcal{O} \subseteq \mathcal{O}(\mathfrak{a})$, so when $\mathcal{O}$ is maximal every nonzero $\mathcal{O}$-ideal is proper.

3. Prove that if $L(a, b, c) = a[1, \tau]$ is the lattice of a form in $F(D)$, then L is a proper $\mathcal{O}$-ideal of norm a, where $\mathcal{O} = \mathcal{O}(L) = [1, a\tau]$. Give an example of an $\mathcal{O}$-ideal that is not proper, thereby proving that not every $\mathcal{O}$-ideal arises as the lattice of a form (or is even homothetic to the lattice of a form).

4. Conversely, prove that every proper $\mathcal{O}$-ideal is homothetic to the lattice of a form in $F(D)$.

The product of two lattices $[\omega_1, \omega_2]$ and $[\omega_3, \omega_4]$ is defined to be $[\omega_1\omega_3, \omega_1\omega_4, \omega_2\omega_3, \omega_2\omega_4]$. In general, the product of two lattices need not be a lattice, but if the lattices are $\mathcal{O}$-ideals, then their product is an $\mathcal{O}$-ideal and therefore a lattice (the lattice product agrees with the usual definition of the product of ideals).

5. Let $\mathrm{cl}(\mathcal{O})$ denote the set of equivalence classes (under homothety) of lattices that are proper $\mathcal{O}$-ideals. Prove that the lattice product makes $\mathrm{cl}(\mathcal{O})$ into an abelian group. Conclude that the corresponding operation on the equivalence classes of $F(D)$ makes $\mathrm{cl}(D)$ into an abelian group that is isomorphic to $\mathrm{cl}(\mathcal{O})$.

To perform explicit computations in $\mathrm{cl}(D)$ we need to translate the product operation on lattices $L(f_1)$ and $L(f_2)$ into a corresponding product operation on forms $f_1, f_2 \in F(D)$. This is known as *composition* of forms, and is performed as follows. If $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ are forms in $F(D)$, then let $s = (b_1 + b_2)/2$ (this is an integer because b_1, b_2 and D all have the same parity). Use the extended Euclidean algorithm (twice) to compute integers u, v, w, and d such that $ua_1 + va_2 + ws = d = \gcd(a_1, a_2, s)$. The composition of f_1 and f_2 is then given by

$$f_1 * f_2 = (a_3, b_3, c_3) = \left(\frac{a_1 a_2}{d^2},\ b_2 + \frac{2a_2}{d}(v(s - b_2) - wc_2),\ \frac{b_3^2 - D}{4a_3} \right).$$

It is a straight-forward but tedious task to verify that this composition formula satisfies $L(f_1 * f_2) = L(f_1) * L(f_2)$; you are not asked to do this.

6. Verify that the inverse of (a, b, c) is $(a, -b, c)$ and that the unique reduced from with $a = 1$ acts as the identity (see Problem 2 for the definition of a reduced form).

Unfortunately, even if f_1 and f_2 are reduced forms, the composition of f_1 and f_2 need not be reduced. In order to compute in $\mathrm{cl}(D)$ effectively, we need a reduction algorithm. Recall the matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ that generate $\mathrm{SL}_2(\mathbb{Z})$.

7. Let f be the form (a, b, c). Compute the forms Sf, $T^m f$, and $T^{-m} f$, for a positive integer m.

A form (a, b, c) with $-a < b \le a$ is said to be *normalized*.

8. Show that for any form f there is an integer m such that $T^m f$ is normalized, and give an explicit formula for m. Let us call $T^m f$ the *normalization* of f. Now let $f = (a, b, c)$ be a normalized form and prove the following:

(a) If $a < \sqrt{|D|}/2$ then f is reduced.

(b) If $a < \sqrt{|D|}$ and f is not reduced, then the normalization of Sf is reduced.

(c) If $a \ge \sqrt{|D|}$ then the normalization (a', b', c') of Sf has $a' \le a/2$.

9. Give an algorithm to compute the reduction of a form f in $F(D)$, and bound its complexity as a function of $n = \log|D|$, assuming that its coefficients are $O(n)$ bits in size. Then bound the complexity of computing the reduction of the product of two reduced forms (this corresponds to performing a group operation in $\mathrm{cl}(D)$).[2]

[2] A quasi-linear bound is known [1], but your bound does not need to be this tight. However it should be polynomial in n.

10. Implement your algorithm and use it to compute the reduction of a form $(a, b, c) \in F(D)$, with a equal to the least prime greater than $|D|^2$ for which $(\frac{D}{a}) = 1$. Do this for the discriminants $D = -103$ and $D = -396$, and for the first three discriminants $D < -N$, where N is the first four digits of your student ID. For the largest $|D|$, list the sequence of normalized forms computed during the reduction.

Problem 4. Survey

Complete the following survey by rating each of the problems you attempted on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found the problem (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			

Also, please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
4/18	Uniformization theorem and CM				
4/23	Orders, ideals, and class groups				

Please feel free to record any additional comments you have on the problem sets or lectures, in particular, ways in which they might be improved.

References

[1] A. Schönhage, *Fast reduction and composition of binary quadratic forms*, in International Symposium on Symbolic and Algebraic Computation–ISSAC'91, ACM, 1991, 128–133.